



October 15, 2003

Ms. Jennifer J. Johnson
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, DC 20551
[Docket No. OP-1155]

Mr. Robert Feldman, Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429

Regulation Comments, Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, DC 20552
[No. 03-35]

Public Information Room
Office of the Comptroller of the Currency
250 E Street, S.W., Mail Stop 1-5
Washington, DC 20219
[Docket No. 03-18]

Re: Interagency Guidance on Response Programs for Unauthorized Access to
Customer Information and Customer Notice
68 Fed. Reg. 47954 (August 12, 2003)

Dear Sir or Madam:

America's Community Bankers ("ACB")¹ is pleased to comment on the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (the "Guidance"). The proposed Guidance has been issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (the "Agencies")².

The Guidance is an extension of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information³ issued pursuant to the Gramm-Leach-Bliley Act (the "GLBA")⁴. The proposed Guidance establishes procedures that would be used to respond to a situation in which a financial institution suspects, or determines that unauthorized individuals have gained access to sensitive customer information maintained in either paper or electronic form.

¹ ACB represents the nation's community banks. ACB members, whose aggregate assets total more than \$1 trillion, pursue progressive, entrepreneurial and service-oriented strategies in providing financial services to benefit their customers and communities.

² 68 Fed. Reg. 47954 (August 12, 2003).

³ 66 Fed. Reg. 8615 (February 1, 2001).

⁴ Pub. L. No. 106-102, Title V, Section 501(b) (November 12, 1999).

ACB Position

The Agencies have outlined many of the basic elements financial institutions should consider in developing a response program. ACB generally supports the efforts of the Agencies to ensure financial institutions are adequately prepared to deal with the unauthorized access of sensitive customer information. We are concerned however that the degree of specificity described in the guidelines may not provide financial institutions with the necessary flexibility to respond effectively to incidents without potentially undermining customer confidence. In summary, ACB suggests the following changes to the Guidelines are necessary:

- The Guidelines should be made more flexible and risk-based;
- Response programs should focus primarily on sensitive customer information;
- Financial institutions should only have to report incidents once;
- Financial institutions should have discretion to determine corrective action; and
- Clarification that the Guidelines apply primarily to retail accounts.

Background

The GLBA Information Security Standards require that all financial institutions establish and maintain an information security program to ensure the security and confidentiality of customer information. As part of these requirements, financial institutions are expected to establish "Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information."⁵ The proposed Guidelines expand on this requirement and propose specific required components of a response program.

As provided in the proposed Guidelines, financial institutions are encouraged to have in place a response program to address the "unauthorized access to, or use of customer information that could result in substantial harm or inconvenience to its customers."⁶ The response program should include corrective measures to respond to unauthorized access to "customer information" and specific procedures for notifying customers whose "sensitive customer information" may have been compromised unless the institution can "reasonably conclude" that misuse of information is unlikely to occur.

Creating a Flexible/Risk-Based Guidelines

ACB urges the Agencies to use the Guidelines as an opportunity to enumerate procedures institutions should consider in developing their response programs and to avoid issuing guidance that is not flexible enough to accommodate changes in a rapidly evolving area. This approach is consistent with the GLBA Information Security Guidelines that describe several security

⁵ 12 CFR Parts 40 (OCC); 208 (FRB); 308 (FDIC); 568 (OTS) Appendix III.C.1.g.

⁶ 68 Fed. Reg. 47958 (August 12, 2003).

measures institutions should consider as part of an information security program⁷ without inadvertently creating a rigid standard by which an institution would be examined against.

Financial Institutions of all sizes and charter types are uniquely dependent on maintaining public trust and have historically taken extraordinary measures to protect the confidentiality of customer information. In the rare event when customer information is compromised, financial institutions are quick to respond to protect their customers, minimize potential loss, and support law enforcement wherever possible. The competitive pressures of today's marketplace demand nothing less. We urge the Agencies to allow financial institutions to develop risk-based response programs that are flexible enough to give institutions the discretion to determine when customer notice is required and avoid prescriptive guidance that may result in a proliferation of costly notices that could create unnecessary customer anxiety or indifference.

Sensitive Customer Information

ACB believes the standard by which the response program is triggered is too low and should be revised to focus primarily on sensitive customer information. The determination as to whether the unauthorized disclosure of information could result in "substantial harm or inconvenience" to a customer is a difficult and subjective analysis. Any financial institution that is confronted with a possible unauthorized disclosure of customer information goes through a difficult assessment process to determine what action is necessary to protect the customer, engage law enforcement, minimize the potential loss, and mitigate potential liability. The definition of sensitive customer information is central to this process.

All of the provisions in the proposed Guidelines apply to any incident involving the unauthorized access to "customer information", except for the customer notice requirements that are only triggered when "sensitive customer information" is compromised. While any incident of unauthorized disclosure will result in a financial institution conducting an assessment of the situation and notifying law enforcement where appropriate, the requirement that accounts be flagged and secured should be required only when sensitive customer information is involved, or at the discretion of the institution.

Additionally, the definition of sensitive customer information should be revised to avoid unnecessarily triggering response programs in situations in which the disclosure of such information is unlikely to result in any fraudulent activity. For example, sensitive information should not include account numbers to non-transactional accounts (e.g., mortgages, secured loans, etc.) where the disclosure of such information provides little risk of unauthorized account access and in some cases may be available in public records. The definition also should be narrowed to exclude encrypted information similar to the requirements of the recently enacted California Security Breach Information Act⁸.

⁷ 66 Fed. Reg. 8639 (February 1, 2001).

⁸ California Civil Code § 1798.29.

Notification of Regulator/Law Enforcement

ACB urges the Agencies and the Financial Institution Crimes Enforcement Network ("FinCEN") to develop procedures to share information in a timely enough manner to avoid duplicative reporting requirements. The Guidelines require that a financial institution notify its primary federal regulator when it becomes aware of an incident involving unauthorized access to customer information that could result in substantial harm or inconvenience to the customer. This notification is in addition to the filing of any Suspicious Activity Report ("SAR") and notification of law enforcement authorities where appropriate.

The SAR reporting requirements contain specific fields for reporting computer intrusion and identity theft related incidents. The SAR reporting instructions for computer intrusion⁹ and supplemental guidance on reporting identity theft cases¹⁰ outline a broad set of scenarios when SAR reports should be filed. It is difficult to imagine any scenario that would trigger the response program without requiring a SAR filing. In an era of increased information sharing among government agencies, financial institutions should not have to report an incident to both their regulator and another government entity. Financial institutions should only be required to report such incidents to FinCEN and the Agencies should rely on FinCEN for notification of such incidents.

ACB also suggests that the Guidance be revised to encourage financial institutions to defer to the recommendations of law enforcement prior to notifying customers of any incident to avoid impeding any criminal investigation. The California Security Breach law¹¹ provides an illustrative example of appropriate exemption language.

Corrective Measures

The Guidelines provide that when a financial institution becomes aware of an incident involving the unauthorized access to customer information that the Agencies expect the institution to "flag" the potentially compromised accounts for increased due diligence, and to "secure" the account until such time that the financial institution and the customer agree on a course of action. Institutions are expected to notify customers only when the unauthorized disclosure of sensitive customer information is involved.

In order to minimize the burden on all financial institutions, ACB urges the Agencies to make the Guidelines more flexible by avoiding overly prescriptive measures and allowing institutions to determine the best course of action for a particular circumstance to protect the customer and the institution. At a minimum, we urge the to revise the corrective measures criteria to apply only to those incidents when sensitive customer information is compromised or the institution determines such measures are appropriate.

⁹ Financial Crimes Enforcement Network; Suspicious Activity Report Instructions (July 2003).

¹⁰ Financial Crimes Enforcement Network; SAR Activity Review, Trends Tips, and Issues (June 2001).

¹¹ California Civil Code § 1798.29(c).

Determination of Course of Action

ACB believes that each financial institution should have the discretion to determine what course of action is appropriate for the situation and respond accordingly. When the unauthorized disclosure of customer information involves information on transactional accounts such as checking account numbers and debit/credit card numbers, the Guidelines provide that financial institutions will secure any compromised account until such time that the "financial institution and the customer agree on a course of action." While financial institutions will attempt to work with their customers to resolve such situations, the Agencies' expectation that an institution should develop a personalized response program to each customer is impractical. This is especially the case in circumstances where a large number of accounts may have been compromised.

Supplemental Guidance/Self-Assessment Tools

ACB suggests that the Agencies develop a self-assessment type questionnaire that would be a part of a regular self-assessment process for financial institutions to determine whether the appropriate corrective measures have been considered to deal with the unauthorized access to customer information.

The potential for unauthorized disclosure of sensitive customer information exists at any financial institution; however, the controls and procedures to deal with such incidents will vary significantly by institution. For example, an institution that does not have an online banking product, or otherwise provide access to the Internet to customer information will not need to be concerned with having procedures in place to immediately reconfigure firewalls and reissue passwords. This self-assessment tool could be a structured questionnaire, or flow-chart, that would allow financial institutions to insure they have considered the appropriate measures to deal with a potential incident. Financial institutions could use this self-assessment tool at a minimum during annual reviews of their overall information security program, or when new products are brought to market.

Scope of Response Programs

ACB believes that the Guidelines should apply only to consumer accounts. As described in the preamble, the Guidelines are an extension of the GLBA Information Security Program requirements and failure to comply with the final Guidance may be treated "as a violation of GLBA"¹². Each financial institution has a unique relationship with its commercial account holders and notification of any security breach and working through any corrective measures for those customers would entail a different process than that of a retail banking account. The Agencies should clarify that the Guidelines do not apply to commercial or agricultural accounts, and that financial institutions should take whatever measures appropriate to address any unauthorized access to business account information and how best to notify business account holders of such an incident.

¹² 68 Fed. Reg. 47955 Section I (August 12, 2003).

Handling Third-Party Disclosure of Sensitive Customer Information

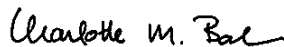
ACB urges the Agencies to allow financial institutions to determine their own course of action when a third party with whom no relationship exists is the source of compromised sensitive customer information. While the Guidelines focus on the unauthorized disclosure of customer information by a financial institution or any service provider engaged to process such data, the most significant breaches of sensitive customer information have been perpetrated against third parties with whom the institution has no relationship. For example, in February 2003, Data Processors International, a company that processes credit-card transactions, had its systems breached and saw computer criminals access the details of over 10 million credit and debit account numbers.

Financial institutions whose customers were affected were notified by the credit card companies shortly after the breach and left to decide on their own what action was appropriate in terms of notifying customers and reissuing credit/debit cards. While to date there has been no reported fraudulent activity relating to any of the affected cards, institutions were left with the task of communicating the breach to their customers and managing the risk associated of an incident they had nothing to do with. In these circumstances, the customer may be notified by multiple entities about this type of breach. Institutions should have the flexibility to determine the most appropriate course of action to protect the customer and mitigate loss.

Conclusion

ACB supports the intent of the Agencies to ensure that financial institutions are adequately prepared to deal with unauthorized access to customer information. We stand ready to work with the Agencies to ensure that the Guidelines are effective without being unduly burdensome or unnecessarily creating customer anxiety or indifference. Thank you for the opportunity to comment on this important matter. Should you have any questions, please contact the undersigned at 202-857-3121 or via e-mail at cbahin@acbankers.org, or Rob Drozdowski at 202-857-3148 or via e-mail at rdrozdowski@acbankers.org.

Sincerely,



Charlotte M. Bahin
Senior Vice President
Regulatory Affairs